REMARKS/ARGUMENTS

Claims 1-20 were pending. Claims 1-20 were variously rejected under 35 USC 102(e) and 35 USC 103(a) in light of Chang or in light and Chang in view of Yatsukawa. Some amendments to the claims were made to clarify the claim scope and are specifically discussed below. Other amendments were made to the claims for stylistic, grammatical, and typographical error correction purposes, and are not made for patentability purposes.

I. THE PRESENT INVENTION

Embodiments of the present invention relate to secure computer network access.

In the Background of the Invention, prior methods to the invention for secure remote access were discuss and have included use of electronic "key cards" or "tokens" to authenticate the client. P. 1, lines 24-28. Drawbacks to such solutions included that these tokens only authenticate the bearer, and not the user. P. 2, lines 1-2. An additional drawback was that these tokens typically need to be manually pre-registered by a network administrator before they are activated. P. 1, lines 31-32. Yet another drawback was that these devices need to be synchronized with the server, otherwise the client will not authenticate. P. 2, lines 3-5.

With embodiments of the present invention, a user does not need to have a hardware or software "token" to gain network access. Instead, the user only needs to have an authentic public/private key pair. In the embodiment illustrated in Figs. 4A-D, the user enters a correct password into a key wallet to retrieve their private key and digital certificate (steps 400-470).

In the various embodiments, the client then requests a one-time password from an external server, step 490. In response, the external server provides the one-time password, which is inactive back to the client, steps 500-530. Accordingly, if any one intercepts the one-time password at this stage, and attempts to gain access to the system, because the one-time password is inactive, the access will be denied. Further, because the one-time password is initially determined, and provided in the challenge, the one-time password should be inactive. Otherwise, a client who receives the challenge will be able to gain access to the network using the one-time password, even though she may be unauthorized.

Notice that before steps 500-530, the client does not have the one-time password. These embodiments allow the one-time password to be freely set, to be different for different users, and to be different for multiple user sessions, and the like. Additionally, these embodiments do not require the user to have any token hardware, to pre-register their client system, or to pre-register user data, as discussed above.

Next, in various embodiments the client uses the received one-time password and digitally signs it with the private key to form a digital data packet (a digital signature), step 540. The digital signature and the user's digital certificate are then sent back to the external server, step 560. Accordingly, data from the external server is signed and then returned to the external server.

Subsequently, if the digital signature and digital certificate authenticate the user, the one-time password is activated, and the client may use the one-time password to access the protected computer network. Steps 570-690. In various embodiments, if the user is not authenticated and the client attempts to use the one-time password to access the network, the access will be denied. Accordingly, the one-time password in the challenge to the client should be inactive until the user is authenticated.

Certain limitations in the disclosed embodiments are recited in the claims.

Claim 14, as amended, now recites, among other limitations, receiving a request for a one-time password in the verification server from a client computer, determining a one-time password within the verification server, wherein the one-time password within the verification server is initially inactive, and communicating data comprising the one-time password that is initially inactive from the verification server to the client computer. Claim 14 also recites activating the one-time password in the verification serer when the user is verified.

Claim 1, as amended, now recites, among other limitations, communicating the challenge from the server to a client computer via a second secure communications channel, wherein the client computer receives the random password from the authentication server that is inactive, and receiving at the server a challenge response from the client computer via the second secure communications channel, wherein the challenge response includes a digital certificate and a digital data packet, wherein the digital certificate includes a public key in an encrypted form, and wherein the digital data packet is determined in the client and comprises a combination of at

least a portion of the challenge and a private key corresponding to the public key. Claim 1 also recites wherein the random password from the authentication server that is inactive is activated when the authentication server verifies the challenge response.

Claim 7, as amended, now recites, among other limitations, receiving challenge data from a authentication server in the client computer via a first secure communications channel , wherein the challenge data comprises a challenge and a password from the authentication server that is inactive, and sending a digital data packet to the authentication server via the external server, wherein the digital data packet is determined in the client computer and comprises a combination of at least a portion of the challenge and the private key. Claim 7 also recites wherein when the authentication server verifies the digital data packet , the password that is inactive is activated.

II. THE CITED REFERENCES

A. Yatsukawa

Yatsukawa relates to an authentication system where seed values Ds0 used to authenticate a user are initially synchronized.

In Yatsukawa, the client / user sets an initial "seed data" Ds0 for authentication purposes in the client and the server, Cols. 15, line 66 - Col. 16, line 12. From Ds0, Dn-1 are subsequently independently generated on a client and a server. In operation, Yatsukawa describes that the client logs into a server, col. 16, lines 46-52. Next, the server sends an authentication-data request, col. 16, lines 54-55. Then, the client generates authentication data D by enciphering the seed data Ds0 by the client private key K, and then D is sent back to the server, col. 16, lines 57-60. The server then deciphers the authentication data D using the client public key K to recover the client seed data. Col. 17, lines 1-14. Next, the server compares the recovered client seed data to the initial seed data previously provided by the user, Ds0. Col. 17, lines 14-17. As illustrated in Fig. 13, block S5, if the recovered client seed data matches Ds0, access is granted.

B. Chang

Chang relates to a token caching security system.

Chang states that one method of reducing remote access security risks is through the use of a "Smart card or Token card." Col. 2, lines 11-13. One such card is disclosed as "the SecurID card commercially available from Security Dynamics, Inc.," Col. 2, lines 13-14. Chang states that the function of the Token card is that it "generates a series of random one-time passwords (OTPs). Col. 2, lines 15-16.

Chang describes that the Token card is used by the user. Specifically, Chang states:

> *To use the Token card, the user typically enters a series of digits and letters displayed on the token-card in the prompt window or inserts the card into a reader that is coupled to the Remote Node. Col. 2, lines 25-28. Emphasis added.*

The series of digits and letters provided by the user is the one time password (OTP). This user-entered OTP is then compared to an OTP independently generated in a password server. Specifically, Chang states:

> *The password server internally generates OTPs in synch with the card. the OTP is then used to verify that the user is allowed to log into the network access server through the remote device ... by comparing the card password to the password server's password at a particular instant in time. Col. 2, lines 28-34. Emphasis added.*

As can be seen, in Chang, the OTP generated by the password server is not ever provided to the user. Instead, the user provides the OTP generated by the Token card to the password server.

Chang notes that use of Token cards by users to generate OTPs is burdensome. More specifically, Chang states:

> *However, a drawback with using OTPs is that additional connections ... are treated as separate connections. Thus, to establish a second session ... the user is required to reenter valid user identification information a second time. Because the OTP is only valid "once", the user must again*

use the token card to obtain another OTP that can be used to validate the second connection. Col. 2, lines 55-60.

In response, the invention in Chang appears to be a way to reduce having the user use the Token card to enter OTPs for each user session. Col. 3, lines 13-17.

In Chang, initially, the user uses a Token card to generate an OTP and then the user provides the OTP to a authenticating server. Specifically, Chang states:

The method comprises the steps of receiving a request to establish a session between the client and the first server, wherein the request includes identification information for authenticating a requesting user. Col. 3, lines 25-29. Emphasis added.

Chang also states that the identification information includes the OTP. Specifically:

One feature of this aspect is that the identification information includes a user name and a one-time password (OTP). col. 3, lines 35-37. Emphasis added.

In response to the user request, an authentication step is performed. If the user is authenticated, the identity information is cached. Specifically,

determining, based on the identification information, whether the session between the client and the first server should be established, if the session between the client and the first server should be established, caching the identification information in memory; and establishing the session between the client and the first server. Col. 3, lines 29-34. Emphasis added.

Chang notes that a second server may be used to determine whether the session should be established. Specifically,

[T]he step of determining whether the session between the client and the first server should be established comprises the step of the first server communicating with a second server to determine whether the OTP is currently valid. Col. 3, lines 37-41.

Additionally, Chang notes that the second server checks whether the identification information is cached therein. Specifically,

> *[C]ommunicating with a second server to determine whether the OTP is currently valid further includes the steps of the second server determining whether the username and the OTP were previously cached in memory; and if the user-name and the OTP were not previously cached in memory, the second server communicating with a password server to determine whether the OTP is currently valid. Col. 3, lines 37-41.*

If the identification information is cached, the cached identification information is checked to see if it is still valid. Specifically,

[C]ommunicating with a second server to determine whether the OTP is currently valid further comprises the step of the second server determining whether the username and the OTP were previously cached in memory; and if the user-name and the OTP were previously cached in memory, determining whether the username and the OTP are still valid. Col. 3, lines 52-58.

This embodiment is repeated in the Detailed Description, on Col. 4, lines 31-67, etc. Importantly, on Col. 6, lines 42-47, Chang describes that in block 302 of Fig. 3A, the user provides a request to establish a session, and the request includes the username and OTP. In TABLE 1, Col. 8, lines 24-32, Chang gives an example, where the user "JOE" submits the request and enters a "username="JOE"," "CHAP password ="ABCD"," and "OTP = "1234" (from hand-held card)."

TABLE 1

Time	Action by user or client	Action by AAA server
-1		The database associated with AAA is configured to allow token caching for user JOE. User Identification Information for JOE is configured to expire based on session expiration and a cache time-out value of "60". A CHAP password of "ABCD" is used to validate the connection.
0	user JOE submits a first request to establish a first session by supplying the NAS with the following information: username = "JOE" OTP = "1234" (from hand-held card) CHAP = "ABCD"	In this example, the AAA server currently has no cached information for user JOE. Thus, the AAA server communicates with a token server to verify the OTP "1234". The AAA server also validates the CHAP password "ABCD".
1	User JOE authenticates successfully.	Authentication is successful. The AAA server stores in its cache the username "JOE" and the OTP "1234". The AAA server also generates and stores session information

Next, on Col. 6, lines 48-50, Chang describes that in block 304 of Fig. 3A, the AAA server determines whether the session should be established based on the "user identification information" received from the user. In TABLE 1, Col. 8, lines 24-31, Chang gives an example, where the AAA server communicated with a token server to verify OTP "1234" and validates CHAP password "ABCD."

The Examiner asserts Col. 7, lines 22-61 as disclosing "the challenge comprising at least a random password that is inactive." The undersigned traverses this assertion. In the cited section in Chang, the OTP is independently generated in the Token card, as well as the AAA server. Nowhere in Chang is there any mention of the OTP being provided to the user from any source other than the Token card.

The Examiner cites Col. 7, lines 55-60 as disclosing "activating the one-time password when the user is authenticated." The undersigned traverses this assertion. In the cited section, Chang merely states that if the CHAP or PAP password entered by the user is correct, the session may be established. There is nothing in Chang that discusses activating a password when the user is authenticated.

The Examiner cites Col. 5, lines 29-44 as disclosing "wherein communicating data comprising the one-time password to the client computer comprises communicating via an external server via a secure communication channel." The undersigned traverses this assertion.

The cited section refers to a network system 108, and a client 102. In Fig. 1, Network access server 104 provides the security interface to network system 108. Accordingly, this section does not disclose any external server on a secure communication channel between network system 108 and client 102.

III. THE CITED REFERENCES DISTINGUISHED

A. Claim 14

The elements of Claim 14 are not disclosed, suggested, or taught by Chang. More specifically Chang fails to teach or disclose: receiving a request for a one-time password in the verification server from a client computer, determining a one-time password within the verification server, wherein the one-time password within the verification server is initially inactive, and communicating data comprising the one-time password that is initially inactive from the verification server to the client computer.

As discussed above, the user in Chang uses a Token card in her possession to obtain a OTP. In contrast, Chang does not disclose receiving a request for a OTP, determining a OTP in the verification server, and providing the OPT to a client, as recited above.

Additionally, Chang fails to teach or disclose: activating the one-time password in the verification serer when the user is verified.

In Chang, the OTP independently determined in the AAA server is not initially inactive. As illustrated above, when the OTP from the Token card and the user simply matches the OTP independently determined in the AAA server, the user session is initiated. The OTP determined in the AAA server is not inactive and then activated, but, once determined, is always active.

Accordingly, because Chang fails to disclose at least the above recited limitations, claim 14 is patentable over Chang.

B. Claim 1

The elements of Claim 1 are not disclosed, suggested, or taught by Chang in view of Yatsukawa. More specifically, the cited references fail to teach or disclose: communicating

the challenge from the server to a client computer via a second secure communications channel, wherein the client computer receives the random password from the authentication server that is inactive.

As discussed above, the user in Chang uses a Token card in her possession to obtain a OTP. Additionally, Yatsukawa states that the user provides initial seed data. In contrast, neither Chang or Yatsukawa disclose an authentication server sending a client computer a password that is inactive, or a client computer receiving a password from a server, as recited above.

Additionally, the cited references fail to teach or disclose: receiving at the server a challenge response from the client computer via the second secure communications channel, wherein the challenge response includes a digital certificate and a digital data packet, wherein the digital certificate includes a public key in an encrypted form, and wherein the digital data packet is determined in the client and comprises a combination of at least a portion of the challenge and a private key corresponding to the public key.

As noted by the Examiner, Chang fails to disclose this limitation. In Yatsukawa, as discussed above, an initial seed data (provided by the user) is digitally signed and provided to the server. In contrast, as recited, a digital data packet including at least a portion of the challenge (from the authentication server to the client computer) is digitally signed and returned. Accordingly, what is sent back to the server in Yatsukawa is different from what is recited.

Further, the cited references fail to teach or disclose: wherein the random password from the authentication server that is inactive is activated when the authentication server verifies the challenge response.

In Chang, the OTP independently determined in the AAA server is not initially inactive. As illustrated above, when the OTP from the Token card and the user simply matches the OTP independently determined in the AAA server, the user session is initiated. The password determined in the AAA server is not inactive and then activated, but, once determined, is always active. Similarly, in Yatsukawa, Ds0 determined in the server is not inactive and then activated, but, once determined, is always active.

Accordingly, because Chang and Yatsukawa fail to disclose at least the above recited limitations, claim 1 is patentable over Chang in view of Yastukawa.

C. Claim 7

The elements of Claim 7 are not disclosed, suggested, or taught by Chang in view of Yatsukawa. More specifically, the cited references fail to teach or disclose: receiving challenge data from a authentication server in the client computer via a first secure communications channel, wherein the challenge data comprises a challenge and a password from the authentication server that is inactive.

As discussed above, the user in Chang uses a Token card in her possession to obtain a OTP. Additionally, Yatsukawa states that the user provides initial seed data. In contrast, neither Chang or Yatsukawa disclose a client computer receiving a password from a server that is inactive, as recited above.

Additionally, the cited references fail to teach or disclose: sending a digital data packet to the authentication server via the external server, wherein the digital data packet is determined in the client computer and comprises a combination of at least a portion of the challenge and the private key.

As noted by the Examiner, Chang fails to disclose this limitation. In Yatsukawa, as discussed above, an initial seed data (provided by the user) is digitally signed and provided to the server. In contrast, as recited, a digital data packet sent to the server includes at least a portion of the challenge (from the authentication server to the client computer). Accordingly, what is sent back to the server in Yatsukawa is different from what is recited.

Further, the cited references fail to teach or disclose: wherein when the authentication server verifies the digital data packet, the password that is inactive is activated.

In Chang, the OTP independently determined in the AAA server is not initially inactive. As illustrated above, when the OTP from the Token card and the user simply matches the OTP independently determined in the AAA server, the user session is initiated. The password determined in the AAA server is not inactive and then activated, but, once determined, is always active. Similarly, in Yatsukawa, Ds0 determined in the server is not inactive and then activated, but, once determined, is always active.

Accordingly, because Chang and Yatsukawa fail to disclose at least the above recited limitations, claim 7 is patentable over Chang in view of Yatsukawa.

D. Claim 15

The elements of Claim 15 are not disclosed, suggested, or taught by Chang for the reasons discussed above for claim 14. Additionally, the cited references fail to disclose wherein communicating data comprising the one-time password that is initially inactive to the client computer comprises communicating via an external server via a secure communications channel.

As discussed above, Chang does not disclose an external server between network access server 104 and client 102.

Accordingly, because Chang fails to disclose at least the above recited limitations, claim 15 is patentable over Chang.

E. Remaining Claims

Claims 2-6, which depend from claim 1 are also believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

Claims 8-12, which depend from claim 7 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

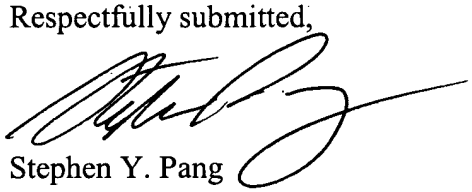
Claims 15-20 which depend from claim 14 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,



Stephen Y. Pang
Reg. No. 38,575

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: (650) 326-2400
Fax: (650) 326-2422
SYP:deh
60408419 v1